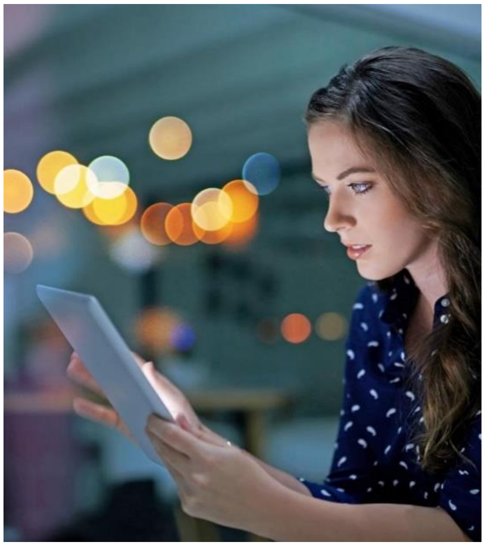
Enable your digital workplace for remote working environments due to coronavirus

March 2020

With the spread of COVID-19, more commonly known as the new coronavirus, within the United States, localities and agencies may take extraordinary measures to protect their employees and shift immediately to a work-from-home or remote work model. For agencies and divisions that do not have established remote worker programs and correlated governance, this sudden transition requires rapid and significant cultural and technical change. Security, data loss prevention, policy and governance, identity and access management, network capacity/bandwidth shifts, and tools that facilitate remote working are all at the forefront when contemplating large scale remote worker support.

During this challenging time, Perspecta is offering an experienced viewpoint using our direct experience supporting and managing our own large remote workforce in anytime, anywhere on any device work environments yields insight that can help other organizations with their own remote work model. This document provides a quick high-level summary of challenges, recommendations and remediation guidance where possible for accelerated large scale remote worker support.



Most agencies have the tools and solutions to support some remote workers, but as agencies have all implemented various suites of digital workplace solutions, the sudden shift to a larger remote work model could pose significant challenges. To help clarify the potential impact in making this type of shift, the following solution categories note remote worker provisions that need consideration for an unexpected workforce shift:

- Plan for the move: policy, governance and inventory
- Internet connections with an internet service provider (ISP)
- Unified endpoint management (UEM), which was previously known as enterprise mobility management or mobile device management
- Unified communications and collaboration
- Enterprise file sharing service (EFSS)
- Virtual desktop infrastructure (VDI)
- Virtual private networking (VPN) infrastructure
- Active Directory (AD)
- Help desk and workplace support

Supporting remote workers—expectations and recommendations

Planning—policy, governance and inventory

It goes without saying that an urgent and unplanned move to a remote workforce requires a look at policy and governance. How digital workplace solutions are configured and used depend on an agency's individual policies and enterprise governance. It's important to understand the risks and be flexible—enough to adjust those policies and governance as necessary throughout the duration of the remote workforce deployment—while still guarding the mission.

Equally crucial is knowing what devices and applications your employees have and use. Our partner, Lakeside Software LLC, uses its SysTrack product to offer a free, cloud-hosted remote work planning solution that can be used to inventory:

- Current device and mobility composition
- Critical applications by user
- Remote work compatibility by user

- Performance baselines
- End-user experience baselines

Internet connections with internet service providers (ISP)

The United States has robust ISP WAN capacity, but the current traffic shifts may cause localized impacts at entry and exit points. Typically, ISP impacts occur at the network edge (access) because their internal network capacity handles both residential and commercial traffic. Companies expanding the remote workforces may need to procure extra bandwidth capacity to data centers or offices containing load balancers and increase load balancer capacity if possible. The backend application servers, already sized for your work population, may need configuration changes to support a remote workforce. If you notice bandwidth impacts, or perceived delays and are unable to configure more bandwidth in these areas, consider having synergistic departments work in shifts.

Unified endpoint management (UEM)

UEM is typically provided by Microsoft Intune (or SCCM, now rebranded together as Endpoint Manager), VMWare Workspace One (legacy Airwatch/Horizon VDI), IBM MaaS360, MobileIron, Blackberry Unified Endpoint Manager (legacy Good for Enterprise), and Citrix Endpoint Management products.

If remote workers are going to use government furnished equipment—such as PCs, laptops and mobile devices—you may already have UEM installed on these devices to manage governance and policy and help prevent data loss. If not, then depending on your policy that supports remote device artifact access, you may need to procure additional licenses to support your newly remote workers. If you use a cloud UEM solution such as Microsoft Intune or VMWare Workspace One, MaaS360 or MobileIron, you should easily be able to add additional capacity support licenses. If you have an on-premise UEM solution, you may need additional UEM application server capacity to support a larger remote workforce.

For workers following a BYOD—or bring your own device—model using their own PCs, laptops, tablets and mobile devices, consider requiring the installation of your UEM solution to those devices for data loss prevention, VPN or VDI solution that complies with your governance and policy.

Unified communication and collaboration

Communication and collaboration solutions are typically sourced from products such as Microsoft Office 365 (including Teams/Skype for Business, Exchange/Outlook, SharePoint), Cisco Unified Communications and Collaboration (with WebEx), Slack, Zoom and Avaya IX Workplace along with a few other niche players.

If you already use one of these products with remote workers, it is easy to continue using this environment and scale it to support your needs. If you have one of these products, but don't currently use it with remote workers, in the interest of time, you may need another option. Likewise, you may need another option if you have an on-premise solution that is difficult to scale, requires architecture changes to support remote workers, or does not support an external workforce, here are some viable options:

- If you have Office 365, G1, G3, G5 or F1 subscriptions, no matter which collaboration solution you currently use, Teams is a good option if you are not currently set up for remote workers. Make sure you enable your Teams licenses for all users
    - To facilitate the ease of Teams adoption, our partner, CoreView, is providing temporary free access to its CoreLearning Microsoft Teams just-in-time short videos to facilitate rapid Teams adoption
- If you don't have Office 365 or not enough Office 365 licenses, procure Office 365 licenses and use Teams for meetings, collaboration and audio/visual conferencing from the Government Community Cloud (GCC), GCC High or DOD Office 365 clouds. Microsoft is ready and scaled to support the influx of new government subscriptions. In fact, Microsoft has begun offering free premium Office 365 usage for new customers for G1 and F1 government subscriptions

- Microsoft has seen an uptick of around 500% with Teams usage on their sovereign Office 365 clouds in Asian countries due to the coronavirus outbreak and was scaled to handle the change
- Microsoft is seeing a dramatic uptick in Teams consumption across commercial and sovereign clouds, but due to the capacity of its hyperscale cloud and the design for the Teams service, they've been able to deliver scale across all environments

Enterprise file sharing service (EFSS)

Ensure remote employees are using OneDrive EFSS to store working files. That way, when your workers return to the office, they can seamlessly continue their work with no delay. Also, OneDrive is instantly replicated across Microsoft's government continental U.S. data centers, so you have immediate high availability.

Virtual desktop infrastructure (VDI)

The main players for VDI are Citrix and VMWare. If your end users currently rely on a VDI solution in their roles, you are set up for remote workers across a VPN and your security is mostly handled. The user experience is dependent upon their edge network/ISP and the bandwidth availability back to your VDI infrastructure. Consider purchasing additional bandwidth for your VDI infrastructure. If you source these solutions from Citrix's or VMWare's VDI cloud, then you don't necessarily need to procure additional bandwidth resources. Please note that each user's home ISP bandwidth can be a factor impacting user experience. Also, make sure your VDI has an enterprise scale backup/archival solution (not to be confused with an EFSS).

If a subset of your employees use VDI for their job and your remaining workforce could also use VDI for their work, consider procuring additional VDI licenses. You may need to scale your on-premise backend VDI servers to prevent performance degradation. If you procure your VDI services from the cloud, scaling to your needs should be supported.

Virtual private network (VPN)

A VPN helps assure security by extending the office network directly to the remote worker. Perspecta recommends that you create a method to install VPN software on any endpoint used by your remote worker. Ideally, you can also provide installation capability from a remote location. If this is not possible, refer to the earlier UEM solutions provided on page three to help mitigate the risk, especially for a BYOD approach.

Depending on the mix of your agency artifacts sourced from your data centers and cloud services, you may need to increase your VPN and load balancer capacity to support remote workers. Ensure your network engineering team has thoroughly assessed the performance bottlenecks and determined if additional network security controls are in place at the Layer 3/4/7 levels, e.g., Domain Name Service (DNS), firewalls, load balancers. The more your workers source resources from the cloud, the better you will be at supporting a large-scale change to a remote workforce. If you source most of your resources from your data center, consider scaling your load balancer and VPN solutions accordingly to support the new volume. However, be sure that any additional network or VPN infrastructure is Federal Information Processing Standard (FIPS) 140-2 compliant and can securely support features and services such as DNS, Network Time Protocol (NTP) and Secure Sockets Layer (SSL) termination at scale.

Active Directory (AD)

Support for remote workers may mean AD changes. If you use AD for access management, you may need to change the worker classification for continued application access. If you source Office 365 currently, your identity and access management solution should already support common access card/personal identity verification authentication or your chosen authentication method with Office 365. If you do not use Office 365 currently and need to quickly adopt it for remote worker usage, there are a variety of authentication options, including an AD federation or synchronization that can occur from your AD to Azure AD. If you do not have enough time to plan for

AD federation or synchronization, you may need to export the appropriate fields and import into Azure AD. Depending on your AD forest, this could be complex. You can import a subset of the AD forest, in this case user and domain list, to get remote workers up and running.

Help desk and workplace support

With a workforce disruption, your users will need help with PC, laptop and connectivity issues. It's important to consider that your help desk agents themselves will now be working remotely. This is in addition to helping your new remote workforce by ensuring the set of services and tools is working optimally.

Support for agents as remote workers

You may already support remote agents with your support services help desk solution. If this is the case, then reconfigure and scale your automatic call distributor and add all agents for a remote work environment. Have your remote agents use your VPN for connecting to your contact center/help desk solution.

If your solution doesn't support remote agents, it is possible to support your end users through Office 365 Teams. Teams can easily be used to troubleshoot end users' PC or laptop problems. If Teams is used in this case, you can set up an agent collaboration team to quickly assist end-user peer agents, enabling accelerated resolution to end-user problems.

Manage remote worker expectations

Set expectations for your employees by creating and issuing a question and answer form that covers at least your plan or method to:

- Support secure VPN connections into the environment
- Set your end user's expectations for performance when working remotely
- Contact the help desk for PC and laptop issues, including connectivity issues
- Support end-user devices that break with a swapping, depot, support model
- Address data loss prevention with instructions
- Support end users' encryption recovery by issuing instructions on storing and retrieving encryption keys
- Patch government furnished equipment machines
- Support any allowed devices, including installation instructions on requisite software agents for policy enforcement

Conclusion

The pandemic coronavirus has created substantial disruptions in our communities and offices. Perspecta is here to help. We have deep expertise in digital workplace solutions and have been managing and supporting large-scale remote workforce populations for decades—internally and for our customers. We offer a full range of advisory, transformation and managed services to support your mission. Visit perspecta.com for more information.